Particularities of security design for wireless networks in small and medium business (SMB)

Nicolae TOMAI, Cluj-Napoca, Romania, tomai@econ.ubbcluj.ro

Small businesses often have small budgets, which often means no fulltime IT staff or no possibility to hire a security consultant to set up a wireless LAN properly. This paper tries to develop a methodology for designing security for wireless networks in SMB.
There are more security options to choose from, when setting up a wireless network, thus the security features needed for a company must be carefully taken in consideration. The benefits from one security feature must be balanced with the implementation and maintenance cost and with the risk of not getting the security level wanted.

Generalities

For all security *projects*, the final goal is strong security. Wireless security functions must be included with those already existing, to give a strong security. Wireless networks, generally, are not an acceptable alternative to wired connectivity in an office, due to the slower speed, shared media, and less secure service than wired networks.
But wireless networking is relatively new and constantly evolving. A number of new protocols are currently being developed by the wireless industry, such as WiMax, (802,16e), 802,11n and ultra wideband. These protocols promise exponentially incrementing wireless networks speeds. The draft standard of 802.11n was finalized and promise speeds 10 times faster than 802.11g and a range up to four times of 802.11g. The news protocols for security like 802.11i allow a good security for wireless networks.

2. The most important phases in deploying wireless networks security

Secured networks involve multiple devices, protocols and standards. We intend to solve this complex problem by identifying some phases which companies can follow to protect against security threads in local wireless networks. These phases would be useful for companies that had decided to integrated WLAN technologies with their own networks and wanted to find the best implementation solution. Also, these can be useful for companies that had already implemented WLAN technologies but were not satisfied by the security degree they had and would like to upgrade, replace or reconfigure their infrastructure so that it would support RSN and other security controls.
To be effective, WLAN security must be considered during the entire life cycle for a WLAN solution. It is recommended that the implementation follows some phases (more or less in number) in designing, deploying and management of a strong security to help companies and organizations. Companies and organizations can have a special methodology for project management which is different, but the methodology tasks and their sequence are probably similar. The most important phases[Fra06] in deploying a wireless network security can be:
1. The initiation phase: This includes the tasks that an organization must perform before beginning to design the WLAN solution: creating a general view about the impact on the organization, creating an implementation strategy, developing WLAN policies and defining functional and business requirements.
2. Acquisition/developing phase. This phase can be divided in:
a. Planning and designing phase. In this phase, network architects specify the technical characteristics for WLAN solution and also the required network components. These characteristics include EAP method or other authentication methods, the protocols used for communication between the access points and the authentication server, access control lists and firewall rules to traffic control, public key infrastructure solution. Another important issue is which users have network access because they can change the security policy. Also, there are providers that

offer support for EAP method and providers that don't offer; there must be ensured that the same security policy can be implemented for all components (users, access points, authentication servers). An expertise on the spot is needed to determine the position and number of access points required and the way these are integrated with the existing cabled network.

b. Procurement phase. This phase consists in indicating the number and type of WLAN components that must be procured, the characteristics for each one, and the licenses needed.

3. Implementation phase. In this phase, the equipments bought are configured to fulfill the operational and security requirements, and then are installed and activated in production. Implementation involves changing the configuration for other security controls and technologies like security events logs, network management, integration of AAA servers and public key infrastructure.

4. Solution maintenance phase. This phase includes tasks related to implementation of effective security on operational system, for instance log system and detection of rouge access points. It is recommended to perform a security audit.

5. Disposal phase. This phase contains new tasks that are defined after the old system or its components are replaced, involving information manipulation for legal requirements or proper disposal.

A wrong implementation of these phases can significantly increase the risk that a WLAN system is compromised. The companies must take into consideration other recommendations and determine their applicability on their own system. Generally, these recommendations increase the security level of standard procedures but they should be avoided if they are not feasible or if the implementation cost is not justified for the risk reduction it offers. The companies must develop WLAN security controls not only based on the following recommendations but also on their own scenarios. Large organizations divide IT work to more teams. For instance, a department can be in charge with PC and laptop support, while other is taking care of the network infrastructure. For these organizations, WLAN implementation requires the participation of more IT support departments.

3. Selecting the Appropriate Security Strategy

Small businesses often have small budgets, which often means no fulltime IT staff and no money to hire a security consultant to setup a WLAN properly.

The goal of any security plan is to deter potential intruders or attackers. Some security experts will tell you that oft-recommended measures such as changing the default SSID, tunning off SSID broadcasting and enabling MAC filtering, but there are ways around each. Other low cost security measures that can be implemented by a small business with a low cost wireless access point WAP include:

- Using static IP addresses and tunning off DHCP on the router or WAP so an unauthorized person can't easily get a valid IP address;
- Positioning the AP to minimize its range so an intruder will be hard to detect AP;
- Tunning the WAP off if you don't need to use wireless network.
- Use a single SSID to provide unified WLAN services[MS05] allowng wireless users the same access to users and allows administrator to apply GPO(Group Policy Objects)

Network service mechanisms built into original WLAN included a PKI (Public Key Infrastructure) that issues certificates via Active Directory.

3.1. Authentication Methods

Choosing the right method for authentication, data encryption and security for ensuring the packets integrity in a wireless LAN network is a consequence of multiple factors. The company' security policies, data type, complexity of the chosen solution are factors that influence the authentication method and data encryption scheme. First of all, the security requirements for wireless LAN networks must be identified. We should answer the question what we want to protect and who should get access to the network. Second, we

must identify the advantages for each authentication method and each data encryption method and the overhead needed for configuration of each security component. Next, we must test the security characteristics that we had chosen for client's hardware and software to check if they satisfy the network requirements. If the results are satisfying, we can start to design network configuration and set up the required components.

The main security is achieved through WPA (Wi-Fi Protected Access). WPA is a standard based on increasing security to increase the data protection level and access control for existing and future LANs.

We also have to change the initial password that was given by the producer.

If it is possible, SSID (Service Set IDentifier) will be blocked. This system consists of a 32 characters identifier which is attached to the header of the packets sent outside WLAN network. This acts like a password when a mobile device tries to connect to the BSS. An SSID is different for one WLAN to another; therefore all the access points and all the devices that are trying to connect to a WLAN must have the same SSID. Because SSID can be recognized in a packet, it does not ensure any security, it only identifies the network. It causes network "isolation" which makes it more difficult to be found by hackers.

Many large companies are using VPN (Virtual Private Network) technology for management staffs that need to access the company's database from the distance. VPN systems are also used for wireless networks. A VPN creates a virtual tunnel from the computer through the access point of the wireless network and then through the Internet till the company's central network. It is complicated and costly to use a VPN for security settings in case we work at home, airports etc.

The most known authentication methods for wireless LAN networks are:

- No authentication method at all
- MAC Address Filtering;
- Shared WEP Key;
- Pre-Shared Key;
- 802.1x;
- 3rd Party VPN Authentication.

Some of these authentication methods can be combined to create more strong security solutions. MAC Address Filtering is a separate authentication method that can be applied to any other authentication method. For instance, for small network implementations, which do not need a complex solution like RADIUS server, we can choose Shared WEP Key combined with MAC Address Filtering as an authentication method for access control. For clients who want a stronger authentication, 802.11x together with EAP technology might be the best solution. This can be combined with MAC Address Filtering when we need a high level security. There is always a discrepancy between a high level security and the utility and ease of network setting and usage. If we use a strong authentication method like 802.1x, we need EAP (Extensible Authentication Protocol). Depending on the company's security requirements, the chosen EAP method can make network usage more difficult, especially when we have EAP-TLS.

The most known EAP types are:

- EAP-MD5;
- EAP-TLS;
- EAP-TTLS;
- PEAP;
- Cisco LEAP.

EAP-MD5 does not offer a security like other EAP methods and it is not recommended for authentication in wireless networks. At the other end, there is EAP-TLS, as one of the best EAP methods. This method requires a unique PKI certification for all the authentication servers and all wireless clients. 802.1x together with EAP-TLS is the most complicated authentication system to use and maintain. The chosen security solution is influencing directly the future hardware and software devices that will be bought.

3.2. Criteria in choosing EAP

For most of the IT projects[Tom06], the total cost for wireless ownership is not just that of hardware devices acquisitions and implementations. Permanent maintenance can be an important component of costs depending on the chosen EAP method and of the wireless solution.

If we use 802.1x, we need EAP. Answering the following questions related to company' security needs, budget and human resources, we will be able to choose the best authentication and encryption methods adequate to the desired network:

a) Do we want to get both users and network (access points) authentication?

Through users and network authentication, we obtain the basic authentication scheme between staff and company's wireless network. In this way the network is protected from the unauthorized users or users from unauthorized networks. In this case, EAP-TLS is the best choice.

b) Is it necessary a strong security for authentication?

The security level used for the exchange of user keys and passwords between client and authentication server must be carefully set up. Strong authentication is good, but in most cases involves high costs for its implementation and maintenance and also strong user knowledge. If we need a strong authentication EAP-TLS, EAP-TTLS, and PEAP are good choices. EAP-TTLS and PEAP are easier to implement than EAP-TLS because client certificates are not required.

c) Does the chosen solution require permanent maintenance?

As the users adopt wireless technology, the time needed for setting up the network and continuous maintenance for each new user will become decisive in choosing the EAP method. EAP-TLS is the safest, but it requires usage of client certificates, increases the setting up and maintenance efforts.

d) Is it important to use unique keys for each user in a session?

If a unique encryption key is necessary for each user in each session, data confidentiality is much more increased than in a static WEP. This can be done using clients and authentication servers which enable 802.1x wireless authentication. Most of the EAP methods can be used for 802.1x with dynamic WEP keys, but the RADIUS servers must be upgraded to be compatible with 802.1x.

e) Is it important to regenerate the encryption key?

Through regeneration of encryption keys at specific time intervals, data confidentiality in wireless networks is much more increased. 802.1x together with WPA and TKIP will enable this. Most of EAP methods can be used for 802.1x with dynamic WEP keys, but the RADIUS servers must be upgraded to be compatible with 802.1x.

f) Can we use the existing user directory?

The required time for implementation can be significantly reduced if the 802.1x RADIUS servers can use the existing LDAP databases or Windows Active Directory. The users will be able to use existing accounts and network usage will not change significantly.

g) Do we need to implement guest (client) access; how many security requirements are?

For wireless connections, which value is more important: usage ease and simplicity or security (for guest access at Hot Spots)? Does it require Web authentication with no WEP key or a simplified WEP key? Wireless LAN networks with low security or no security at all should be clearly separated from the usual data traffic in a company by using VLAN or separate connections to the Internet or DMZ (Demilitarized Zone). It is necessary to use firewalls, monitoring and intrusion detection systems (IDS).

3.3. Data encryption methods

After selecting an authentication method for WLAN, we will have to choose data encryption scheme to protect packets transmitted through air way. Some of these encryption schemes can be used only with specific authentication methods. Not all wireless network cards can support the newest and the strongest security standards. If we already have NIC cards, these must be checked with the producer to determine whether there are updated drivers so that cards could operate with the selected security solution. In case security options can not be implemented, NIC cards must be changed (bought new ones).

Not all operating systems can work with the newest encryption methods. For instance, WPA is not supported in default mode for all Microsoft or UNIX operating systems. Therefore, if WPA was chosen as the com-

pany's data encryption standard, we must procure new 802.1x client systems. Any of the authentication methods can be combined with a data encryption method to get WLAN network security.Some of the most known data encryption schemes available for wireless networks are:

- No encryption at all;
- Static WEP;
- Dynamic WEP, Rotating WEP;
- WiFi Protected Access (WPA with TKIP and AES-CCM);
- 3rd Party VPN Encryption.

4. Wireless networks division in work domains

Most of the companies' wireless networks implementations consist in one or more AP in a wireless domain, which is the wireless network name. A wireless domain is a continuous wireless service with the same SSID or ESSID. Wireless users will be able to view on their wireless devices the domain's networks available, and the network card will automatically connect to the best AP from the wireless network. Depending on company's wireless network strategy, domains can be set up for grouping the wireless networks at each building, floor, department or other criteria.

If the company's internal LAN strategy[Ole04] permits full access to all internal network areas, an internal network domain for the whole building or a level 2 subnetwork is a good starting strategy. On the contrary, if the internal LAN strategy is to separate, monitor, and control the network traffic for each department (or other criteria), it is required to create more network domains, different for each department or traffic segment. It is recommended to use divisional and management strategy from wired networks to wireless networks as well, for consistency in security policies.

The advantage of a single network (or a single domain) in a building or at a single floor is easy planning and usage for users. This strategy … access control for any client because each wireless network can have a single ID VLAN attribute. If more departments are using the same wireless network (domain), there is no possibility to control access for each user using VLAN. Some modern wireless solutions offer user policies and dynamic VLAN to compensate and to allow RADIUS server to describe VLAN settings and user policies based on user credentials.

Another strategy is creating a single wireless network (a single domain) for each security requirement that the company has for wireless users. An example of this strategy is creating a very secured wireless network (domain) for employees, and another one with lower security for guests or clients users. The wireless network (domain) for the employees can be identified using a descriptive SSID (for instance, ABuilding-1Floor) and can be secured using 802.1x and WPA. The wireless network (domain) for guests can be identified using an obvious SSID like "Guests" and can be secured with a simple WEP key and Web authentication using an generic identifier and a password.

5. Conclusions

Wireless Networks provide new challenges for security and network administrators that were not met in wired networks. Best practices propose an adequate level structure for network security. The configuration of access points, firewalls and VPNs should be considered. Security strategies should be defined for an acceptable performance level and the intrusion detection system for wireless networks should eliminate the security problems and assure that what we believe is secured is indeed secured.

References

[Fra06], S. Frankel, B. Eydt, L. Owens, K. Kent, Guide to IEEE 802.11i: Establishing Robust Security Networks, NIST Special Publication 800-97.

[Gas05] Mattew Gast, 802.11 Wireless Networks, The Definitive Guide Networks, O'Reilly, 2005.

[MS05], Microsoft IT, Technical Case Study, Published: August 3, 2005

[Ole04], Ron Olexa, Implementing 802.11, 802,16 and 802.20 Wireless Networks: Planning, Troubleshooting and Maintenance, Publisher, Paperback, ISBN 0750678089, 2004

[Tom06], N. Tomai, C. Tomai, Reţele de calculatoare fără fir, elemente de proiectare, Ed. Risoprint, ISBN: 973-751-361-4, 978-973-751-361-8, 296 pagini.
[***] "Building Secure Wireless Local Area Networks", a white paper by Colubris Networks Inc.
[***] "Cisco Aironet Security *Solution Provides* Dynamic WEP *to Address* Researchers'Concerns",
http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1281_pp.htm
[***] "Overview Wireless LAN Security The Growth of Wireless LANs",
http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm
[***]A Comprehensive Review of 802.11 Wireless LAN Security and the Cisco Wireless Security Suite"; Cisco Press
[***]Methodology for Testing Wireless LAN Performance, White Paper, 2003 – Atheros Communications ,www.atheros.com
[***06], Wireless Networking inthe Developing World, 2006, Limehouse Book Sprint Team
[***] "Building Secure Wireless Local Area Networks", a white paper by Colubris Networks Inc.
[***]"Cisco Aironet Security *Solution Provides* Dynamic WEP *to Address* Researchers' Concerns",
http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1281_pp.htm
[***] "Overview Wireless LAN Security The Growth of Wireless LANs",
http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm